Amendments to the Claims

This listing of claims will replace all prior version, and listings, of claims in the application.

Listing of Claims:

1. – 8. (Canceled)

9. (Currently Amended) A transaction device, comprising:

an inputting means for receiving an inputted identification verification data directly from a user;

a decoder coupled to the inputting means for sensing, decoding, and verifying the inputted identification data, wherein the inputted identification verification data is not shared with another device; and

a processor coupled to the decoder, wherein the decoder asserts an activation signal to the processor if the identification verification data is verified, wherein the decoder de-asserts the activation signal when an event occurs.

10. (Original) The device of claim 9, wherein the event comprises a completion of a secure transaction.

11. (Original) The device of claim 9, further comprising:

a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires.

12. (Original) The device of claim 9, wherein the inputting means comprises a plurality of capacitive keys, wherein each capacitive key comprises a first side and a second side.

13. (Original) The device of claim 9, further comprising:

an oscillator coupled to the inputting means; and

a power source coupled to the oscillator and the decoder.

14. (Original) The device of claim 9, wherein the decoder comprises a stored identification verification data, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data.

15. (Currently Amended) A transaction device, comprising:

a plurality of capacitive keys for inputting an identification verification data directly by a user, wherein each capacitive key comprises a first side and a second side;

an oscillator coupled to the first side of each capacitive key;

a decoder coupled to the second side of each capacitive key for sensing, decoding, and verifying the inputted identification verification data when the first and second sides of at least one of the capacitive keys are coupled, wherein the decoder comprises a stored identification verification data, wherein the stored identification verification data is not shared with another device, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data;

a power source coupled to the oscillator and the decoder;

a processor coupled to the decoder, wherein the decoder asserts an activation signal to the

processor if the inputted identification verification data is verified; and

a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires.

16. (Currently Amended) A transaction device, comprising:

a plurality of capacitive keys for inputting an identification verification data directly by a user, wherein each capacitive key comprises a first side and a second side;

an oscillator coupled to the first side of each capacitive key;

a decoder coupled to the second side of each capacitive key for sensing, decoding, and verifying the inputted identification verification data when the first and second sides of at least one of the capacitive keys are coupled, wherein the decoder comprises a stored identification verification data, wherein the stored identification verification data is not shared with another device, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data;

a power source coupled to the oscillator and the decoder; and

a processor coupled to the decoder, wherein the decoder asserts an activation signal to the processor if the inputted identification verification data is verified, wherein the decoder de-asserts the activation signal to the process when a secure transaction is completed.

17. (Previously Presented) A method for providing a secure transaction, comprising the steps of:

(a) receiving an inputted identification verification data by a transaction device

directly from a user;

(b) sensing, decoding, and verifying the inputted identification verification data by a decoder of the transaction device, wherein the new identification verification data is not shared with another device; and

(c) asserting an activation signal to a processor coupled to the decoder if the identification verification data is verified, wherein the decoder de-asserts the activation signal when an event occurs.

18. (Previously Presented) The method of claim 17, wherein the receiving step (a) comprises:

(a1) assigning an initial identification verification data to the user;

(a2) receiving the initial identification verification data by the transaction device directly from the user;

(a3) verifying the initial identification verification data by the transaction device;

(a4) receiving an indication of a new identification verification data by the transaction device; and

(a5) receiving the new identification verification data by the transaction device directly from the user.

19. (Previously Presented) The method of claim 17, wherein the asserting step (c) comprises:

(c1) determining if the inputted identification verification data matches a new identification verification data stored at the transaction device;

(c2) asserting the activation signal if the inputted identification verification data matches

the new identification verification data; and

(c3) starting a timer if the activation signal is asserted, wherein the timer expires after the predetermined period of time.

20. (Previously Presented) The method of claim 19, wherein the asserting step (c) further comprises:

(c4) de-asserting the activation signal when the timer expires.

21. (Previously Presented) The method of claim 19, wherein the asserting step (c) further comprises:

(c5) de-asserting the activation signal when the secure transaction is completed.

22. (Previously Presented) The method of claim 19, wherein the new identification verification data comprises at least one of the following:

a personal identification number;

a fingerprint; or

a signature.